

What's Wrong with Your pa\$\$w0rd?



https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_password?language=en

OCT 23, 2015 • VOLUME 04 • ISSUE 01

Research is currently underway to explore ways to create more effective passwords and even how to store a password in someone's mind that they can't directly recall – for example, by teaching them to play a song and measuring their reaction times.

How Do You Choose Your Passwords?

Do you start with a capital letter? If forced to include a number, do you choose the number 1? Or an exclamation point “!” if forced to include a special character? If so, you’re not alone.

Studying passwords has recently become an active area of research. Specialists in disciplines ranging from computer science and cryptography to behavioral science and psychology are working to understand how people choose and use passwords and how to make them stronger and more secure.

These researchers study things such as the average number of passwords and average number of accounts each user has, how many passwords the user types per day, how often passwords are shared among sites, and how often they are forgotten. They also analyze detailed data on password strength, the types and

lengths of passwords chosen, and how they vary by site.

As a result of this work, we know that the word “password” was the most common password until recently, when it was surpassed by “123456.” “Monkey” is the most popular password related to animals (and the 14th most common password overall).

It's tempting to create simple passwords so that you can remember them easily. The problem with simple passwords is that they are easy for hackers to crack. Strong passwords often include a mix of capital and lower case letters, numbers, and special characters. Developing passwords that include unexpected sequences can improve your security and help to avoid dictionary attacks (attempts to decipher passwords trying words in a dictionary).



Lorrie Faith Cranor is a Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. There, she is director of the CyLab Usable Privacy and Security Laboratory (CUPS) and co-director of the MSIT-Privacy Engineering masters program. She is also a co-founder of Wombat Security

Who does this stuff ?

Technologies, Inc., a company that provides information security awareness and training software. She has combined her passion for privacy and security, computers, and technology with quilting. In her free time, she practices yoga and spends time with her family and three children.



Photo by Scott Schiller

The case for security

While the combination lock dates back to the early Roman era, the modern combination pad lock was invented in 1878 by Joseph Loch for Tiffany's Jewelers in New York City. Today, people use combination pad locks because of the convenience and security they offer. Using a combination of letters and numbers, pad locks help people secure valuable items. In the information age, passwords serve a similar purpose. They allow people to interact securely over the internet. Passwords allow people to keep personal information private, save progress after playing online games, and safely shop online. Knowing how to create strong passwords can keep your information.

Discuss

- What do passwords do?
- How are passwords helpful?
- What could you do to make your password extremely strong?
- Since experts suggest you should never write your password down, what strategies can you use to make sure you remember your password?

My Password

Choose a stronger password by selecting letters from a phrase or song.

For example, take the first letter from each word and the numbers from the following phrase:

CS Bits and Bytes 2015 is awesome!

creates the password:
CSB&B2015ia!

Learn More

Powerful Passwords Lesson Plan



http://www.cherokeek12.org/files/2012/05/5-LP-Powerful_Passwords.pdf

Test Your Password Strength



<http://www.passwordmeter.com>

About Lorrie Cranor



<http://lorrie.cranor.org>

Creating Strong Passwords You Can Remember



<https://www.us-cert.gov/ncas/tips/ST04-002>

About

CS Bits & Bytes is a bi-weekly newsletter highlighting innovative computer science research. It is our hope that you will use CS Bits & Bytes to engage in the multi-faceted world of computer science to become not just a user, but also a creator of technology. Please visit our website at: www.nsf.gov/cise/csbytes.

